• Un rastreador en tu bolsillo •

Fundación Karisma

Resumen ejecutivo

El robo de celulares es un problema que, desde el 2011, el gobierno colombiano ha querido solucionar a través del sistema de registro de celulares[1]. La idea del sistema, impulsado por el gobierno nacional y la Comisión de Regulación de Comunicaciones (CRC), es bloquear los celulares reportados como robados o perdidos a partir de un número identificador único de cada aparato, llamado IMEI. Idealmente, el hecho de que un celular reportado no funcione en ninguna red en Colombia debería disminuir el hurto. Sin embargo, el sistema, tal y como existe actualmente excede ese alcance y afecta de tal forma los derechos fundamentales a la intimidad y a la libertad de expresión que no se justifica su existencia, aún si fuera efectivo.

“Un rastreador en tu bolsillo” presenta un análisis del sistema de registro de celulares para combatir el hurto. El análisis está dividido en tres partes:

1. Una descripción básica de cómo funciona el sistema.
2. Puntos problemáticos del sistema.
3. Conclusiones y recomendaciones para los principales actores involucrados en el sistema: la CRC, el Ministerio de las TIC, la Autoridad de Protección de Datos y los operadores de telefonía móvil.

[1] Este sistema está estructurado por el Artículo 106 de la Ley 1453, el Decreto 1633 y la Resolución CRC 3128. Todas estas normas aparecieron en 2011.

¿Cómo funciona el sistema? Los elementos básicos del sistema de registro

IMEI y bases de datos

El IMEI es un número único asignado a cada celular. Los operadores móviles pueden usar este número para saber qué celular quiere usar la red. Cuando una persona reporta que le han robado su celular o que se ha perdido, el operador registra el IMEI de ese celular en una base de datos particular, llamada *base de datos operativa negativa*, y le niega a ese IMEI los servicios de la red. Es decir, el celular no puede recibir ni hacer llamadas ni enviar mensajes de texto.

Adicionalmente, cuando una persona adquiere un celular, está obligada a entregar su información personal para que el operador la registre junto con el IMEI del celular, el número con el que se identifica la suscripción con el operador (IMSI) y el número de la línea (MSISDN). Esta información queda guardada en la *base de datos operativa positiva* que lleva cada operador.

El sistema de registro también tiene otro tipo de base de datos (BD), llamada *BD Administrativa*, que actualmente es operada por El Corte Inglés, una empresa de origen español. Esta empresa lleva dos tipos de bases de datos: negativa y positiva. En la primera, llamada *BD Administrativa negativa*, recoge todos los IMEI de los celulares reportados y los comparte con los operadores que no recibieron el reporte de la persona usuaria. Así, cada operador tiene la lista de todos los celulares reportados, sin importar si le fueron reportados directamente a él o a otro operador. En la segunda, la *BD Administrativa positiva*, están recogidos los mismos datos que existen en cada una de las BD positivas de los operadores.

Procedimiento de verificación

Para asegurarse de que ningún celular reportado o no registrado en la BD positiva funcione, el sistema tiene un procedimiento que busca verificar periódicamente que sólo los celulares autorizados hayan utilizado la red. Este procedimiento, que se divide en dos etapas o ciclos, detecta IMEI irregulares, aparte de los reportados. Por ejemplo, en la verificación los operadores deben encontrar si a sus redes se conectaron IMEI que no cumplen con los estándares técnicos; si hay IMEI no registrados en la BD positiva o si hay

casos donde se puede sospechar que el IMEI original de un aparato fue duplicado o clonado en otro.

Para hacer posible el procedimiento de verificación, los operadores deben analizar información sensible sobre las personas. Esta información está contenida en los *registros de detalle de llamadas* (CDR en inglés), que muestran con quién, dónde, por cuánto tiempo se comunica la persona suscriptora del servicio de telefonía móvil. Concretamente, la CRC ordena a los operadores analizar, entre otros, la siguiente información de cada persona:

- Número emisor y receptor de la llamada
- Ubicación de la llamada o sesión de datos
- Hora y duración de la llamada o sesión de datos
- IMEI
- IMSI

Cuando se detecta que un celular con IMEI reportado o irregular usó las redes móviles, el operador debe bloquear el IMEI.

Puntos problemáticos del sistema

El marco de este análisis es el Derecho Internacional de los Derechos Humanos, tanto del sistema universal como del interamericano, como también de la Constitución Política. Así mismo, se tienen en cuenta los *Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones.*[2]

Los problemas que representa el sistema para los derechos a la intimidad y a la libertad de expresión son analizados a partir de los elementos del sistema, es decir, las bases de datos y el sistema de verificación. Finalmente, se hacen unas observaciones sobre el sistema en general.

[2] *Principios Internacionales sobre la aplicación de los Derechos Humanos a la vigilancia de las comunicaciones.* (2014, 10 de mayo). Disponible en https://necessaryandproportionate.org/es/necesarios-proporcionados.

Problemas asociados a las bases de datos del sistema de registro de celulares

Cada IMEI está atado a una persona: Por la manera como funciona el registro, cada IMEI, en últimas, equivale a la identidad de una persona. Estos mecanismos de registro han sido rechazados por la Relatoría Especial para la libertad de expresión de las Naciones Unidas porque eliminan la posibilidad de comunicarse anónimamente, permiten el rastreo y la ubicación de las personas y porque simplifican la vigilancia de las comunicaciones.

Acceso de autoridades: Según la regulación, cualquier autoridad puede acceder a la información de las bases de datos de IMEI. Sin embargo, según la Constitución, es claro que este acceso debe estar autorizado por un juez, y solo para casos de investigación penal. Sin embargo, es problemático que el Ministerio de las TIC y la CRC hayan establecido en la regulación de forma tan ambigua el acceso a esta información de forma tan ambigua.

Precisamente, el abuso de esta información es el principal peligro al que se enfrentan las personas en Colombia que tienen una suscripción de telefonía móvil. En México, se creó un sistema similar al colombiano, pero en 2011 fue eliminado porque se descubrió que los datos de las personas eran vendidos y se usaban para fines ilegales como la extorsión y el secuestro. En Ucrania, las personas que participaron de una protesta en 2014 recibieron un mensaje del texto que decía "Querido suscriptor, ha sido registrado como participante en un motín". En Colombia, con este sistema, las autoridades no solo podrían obtener los teléfonos de las personas reunidas en un determinado lugar, sino también sus nombres, cédulas y direcciones físicas, entre otros, justamente, porque tienen acceso a una base de datos que relaciona los datos técnicos del celular con información personal de la persona usuaria.

Problemas derivados del procedimiento de verificación de IMEI

El procedimiento de verificación de IMEI usa datos muy sensibles de las comunicaciones de las personas suscriptoras, conocidos generalmente como "metadatos de las comunicaciones", que suelen estar en los registros de cuenta o CDR. Estos datos revelan a dónde se llama, cuándo, desde dónde y por cuánto tiempo. Por su naturaleza, sirven para crear perfiles completos de las actividades y preferencias de una persona.[3]

---

[3] *Principios internacionales…, op. cit* (nota 2).

Por su importancia, se ha reconocido internacionalmente que la recolección y conservación de metadatos son una forma de limitar el derecho a la intimidad. Es importante proteger esta información porque con ella se pueden descubrir patrones y dar una idea del comportamiento de las personas[4], especialmente cuando se pueden cruzar y agregar varias fuentes de información.[5] Es necesario, entonces, considerar que la producción y retención de metadatos de las comunicaciones aumentan la capacidad de vigilancia del estado y, por la misma vía, la posibilidad de abusar de esa información.[6]

La regulación del sistema de registro de celulares no tiene en cuenta el contexto de la vigilancia de las comunicaciones y, por tanto, no tuvo en cuenta los riesgos que implica para los derechos a la intimidad y a la libertad de expresión. En Colombia existen medidas como la interceptación de comunicaciones y la retención de datos de comunicaciones móviles que no respetan los límites que impone la protección de los derechos mencionados.[7] Aún así, estas medidas usan los metadatos de las comunicaciones sin los controles adecuados para evitar el abuso de estas facultades.

La Constitución, que prevalece sobre cualquier otra norma, exige para acceder a las comunicaciones privadas de una persona: (1) que haya una ley que lo permita, (2) que haya

[4] El Alto Comisionado de las Naciones Unidas para los Derechos Humanos, en su informe titulado *El derecho a la privacidad en la era digital*, ha señalado que, desde el punto de vista del derecho a la privacidad, "[l]a agregación de la información comúnmente conocida como 'metadatos' puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada". Consejo de Derechos Humanos. (2014, 30 de junio). A/HRC/27/37, párr. 19.

[5] Human Rights Council, *op. cit.* (nota 3), párr. 15.

[6] Ibid, párr 67.

[7] Para ampliar la información sobre la vigilancia de las comunicaciones en Colombia, pueden consultarse los siguientes documentos: Cortés, C. (2014). Vigilancia de las comunicaciones en Colombia. Bogotá, Colombia: Dejusticia, 18; Rivera, J.C. y Rodríguez, K. (2015). Vigilancia de las comunicaciones por la autoridad y protección de los derechos humanos en Colombia. San Francisco, EEUU: Electronic Frontier Foundation; Castañeda, J.D. (2016). ¿Es legítima la retención de datos en Colombia?. Bogotá, Colombia: Fundación Karisma; Pérez, G. (2016). Hacking Team: malware para la vigilancia en América Latina. Santiago, Chile: Derechos Digitales.

un procedimiento en la ley para realizarlo, y (3) que un juez supervise el procedimiento.[8]

La misma protección que se reconoce al contenido de las comunicaciones debe concederse a los metadatos. Por estas razones, solo la Fiscalía, para recoger pruebas en medio de una investigación penal, puede interceptar las comunicaciones de una persona o acceder a las bases de datos que contienen información sobre sus comunicaciones. Esta actividad requiere autorización judicial. Toda otra intervención en las comunicaciones personales es inconstitucional.[9]

Problemas del sistema en general

El sistema de registro de celulares en Colombia está diseñado de manera tal que la responsabilidad del sistema recae en un tercero, cuya relación está determinada por un contrato con los operadores. Por tanto, no está sometido a los mismos controles que las entidades públicas. De ahí que haya menos transparencia y menos control democrático.

Un efecto de este sistema es que ni el Ministerio de las TIC ni la CRC conocen el contrato celebrado por los operadores con Informática El Corte Inglés, la empresa elegida para administrar la BDA. Si el contrato no es conocido por ninguna autoridad, claramente no se está controlando el desarrollo del sistema de registro, a pesar de las amplias facultades de intervención del Estado en las telecomunicaciones y de las facultades específicas del Ministerio TIC y la CRC.[10]

Adicionalmente, la ley asignó a la CRC la función de regular un sistema que busca reducir el hurto de celulares cuando esta entidad existe para un fin completamente distinto, que es promover la competencia en las telecomunicaciones.[11]

---

[8] *Constitución Política*, artículo 15. Corte Constitucional (1993). Sentencia T-349. M.P. José Gregorio Hernández Galindo. Disponible en: http://www.corteconstitucional.gov.co/relatoria/1993/T-349-93.htm.

[9] Por ejemplo, la CRC exige recibir de los operadores los CDR de sus suscriptores. *Véase* Resolución CRC 3128 de 2011, artículo 10.a.9, literales b y d.

[10] Ley 1341 de 2009, Artículo 4.

[11] Ibid.

Conclusión: El sistema de registro no es proporcional

El sistema de registro de celulares tiene como objetivo desincentivar el hurto de equipos. Sin embargo, hay varias razones por las cuales el programa no cumple su propósito y, en cambio, constituye una vulneración a los derechos a la intimidad y a la libertad de expresión.

No sirve porque después de ser bloqueado, un celular puede venderse por piezas. Además, el bloqueo sólo impide que el celular funcione en las redes, lo que significa que puede servir como reproductor de música o como una tablet, aún puede hacer llamadas por internet.

> *El sistema se ha ido modificando constantemente para asegurar que no haya ningún celular irregular funcionando en las redes móviles del país. Sin embargo, el IMEI de un celular puede ser alterado, por lo cual siempre se escaparán del control algunos celulares. También es posible vender el celular robado por piezas, actividad contra la cual el sistema de registro no puede hacer nada.*

Aún si fuera efectivo la restricción a los derechos a la intimidad y a la libertad de expresión, el sistema no es proporcional.[12] Por esa razón, el diseño del sistema debe tener en cuenta que no puede, por sí solo, acabar con la cadena criminal que busca combatir. Algunas alternativas, como el reporte voluntario de los celulares robados así como la cooperación entre operadores para bloquearlos, o el seguimiento y captura de bandas criminales dedicadas a este actividad ilegal, pueden resultar más efectivas y menos invasivas para las personas.

---

[12] De acuerdo con cifras oficiales, la cifra de hurto ha aumentado desde el 2011, año en el que entró a funcionar el sistema de registro. El Sistema de información estadístico delincuencial, contravencional y operativo de la Policía (SIEDCO) reportaba más de 32 mil robos para 2011. Esta cifra ha aumentado hasta llegar a más de 52 mil casos en 2015. Ver también: Roa, L. (2016). Extinción de dominio como herramienta contra el hurto de celulares en la ciudad de Bogotá. *Revista Criminalidad*, 58 (2): 157-174. Disponible en http://www.scielo.org.co/pdf/crim/v58n2/v58n2a06.pdf.

Desde el punto de vista de los estándares internacionales de protección de derechos humanos, es claro que **el sistema no es legal ni proporcional, a pesar de que busque un objetivo legítimo**.

Recomendaciones

El sistema de registro de celulares en Colombia es ilegal por las razones vistas anteriormente. Sin embargo, las normas que lo sustentan tienen presunción de legalidad, lo que significa que es necesario que un juez las declare ilegales. Sin embargo, considerando el impacto del sistema para las personas, sin necesidad de intervención judicial, la CRC y el Ministerio TIC pueden eliminar y modificar ciertas partes problemáticas del sistema.

Comisión de Regulación de Comunicaciones

La CRC tiene un papel restringido en el sistema de registro. Sin embargo, puede eliminar algunos puntos problemáticos como la asociación IMEI, IMSI y número de teléfono, la obligación de los operadores de verificar la identidad de las personas usuarias en la Registraduría Nacional y centrales de riesgo financieras y el acceso a las bases de datos por parte de cualquier autoridad sin establecer controles y circunstancias que justifiquen el acceso.

Así mismo, puede eliminar el procedimiento de verificación y el artículo que permite a la propia CRC acceder a los metadatos de las comunicaciones.

Ministerio de las TIC

El Ministerio puede derogar el Decreto 1630 de 2011 en lo que tiene que ver con las bases de datos y el procedimiento de verificación y proponer al Congreso derogar el artículo 106 de la Ley 1453 que asigna la función de regulación del sistema de registro de celulares a la CRC.

Además, debe pensar las políticas públicas relacionadas con tecnología teniendo en cuenta el impacto a los derechos humanos, especialmente a la intimidad y a la libertad de expresión. El Ministerio puede buscar el apoyo de la Corte Interamericana de Derechos Humanos y solicitarle una opinión sobre la compatibilidad del registro de celulares con la

Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos[13].

Finalmente, debe fortalecer alternativas al registro de celulares que no afecten de forma exagerada los derechos a la intimidad y a la libertad de expresión.

Autoridad de Protección de Datos

La Autoridad debe participar en las iniciativas del gobierno que tienen que ver con recolección y uso de datos personales. Esta participación tiene que estar enfocada en la protección de los derechos a la intimidad y al habeas data.

Operadores de telefonía móvil

Los operadores deben revisar las solicitudes de las distintas autoridades y acceder solo a aquellas que están en el marco de la Constitución y la ley. En el mismo sentido, deben publicar informes de transparencia donde se pueda conocer qué información piden las autoridades, para qué y si se aceptó o rechazó la solicitud.

Por último, deben considerar también los derechos fundamentales de las personas usuarias cuando participen en las discusiones con el gobierno y con el regulador. La intervención de Tigo sobre los problemas que el procedimiento de verificación trae para el derecho a la intimidad es un buen ejemplo.

El informe *Un rastreador en tu bolsillo*. Análisis del sistema de registro de celulares en Colombia hace parte de la campaña *No más celus vigilados* que realiza la Fundación Karisma. El texto completo puede descargarse en el sitio web www.karisma.org.co/nomascelusvigilados

[13] Convención Americana sobre Derechos Humanos. Artículo 64. Numeral 2. Reglamento de la la Corte Interamericana de Derechos Humanos. Artículo 72 y ss.